



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/635,882	08/05/2003	Alpesh Patel	CISCP334/6994	1592
22434	7590	08/20/2007	EXAMINER	
BEYER WEAVER LLP			HOFFMAN, BRANDON S	
P.O. BOX 70250			ART UNIT	
OAKLAND, CA 94612-0250			PAPER NUMBER	
			2136	
			MAIL DATE	
			DELIVERY MODE	
			08/20/2007	
			PAPER	

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Application No.

10/635.882

Applicant(s)

PATEL ET AL.

Examiner

Brandon S. Hoffman

Art Unit

2136

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 13 June 2007.
2a) ☒ This action is **FINAL**. 2b) ☐ This action is non-final.
3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1-4,6-31 and 33-54 is/are pending in the application.
4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 1-4,6-31 and 33-54 is/are rejected.
- 7) ☐ Claim(s) _____ is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on _____ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some * c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
2. ☐ Certified copies of the priority documents have been received in Application No. ____.
3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- 1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO/SB/08)
Paper No(s)/Mail Date 6-18-07.

- 4) ☐ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____.
- 5) ☐ Notice of Informal Patent Application
- 6) ☐ Other: _____.

DETAILED ACTION

1. Claims 1-4, 6-31, and 33-54 are pending in this office action, claims 5 and 32 are canceled and claim 54 is newly added.
2. Applicant's arguments, filed June 13, 2007, have been fully considered but they are not persuasive.

Information Disclosure Statement

3. The information disclosure statement (IDS) submitted on June 18, 2007, is in compliance with the provisions of 37 CFR 1.97. Accordingly, the information disclosure statements are being considered by the examiner.

Claim Rejections - 35 USC § 102

4. Claims 1-10, 13-36, and 38-53 are rejected under 35 U.S.C. 102(a/e) as being anticipated by Yokote (U.S. Patent Pub. No. 2002/0147820).

Regarding claims 1 and 45-47, Yokote teaches in a server adapted for authentication, authorization, and accounting, a method/computer-readable medium/server of generating a shared key between a Home Agent and a Mobile node, comprising:

- Receiving a request message from a Home Agent, the request message identifying the Mobile Node (fig. 6, ref. num S6-2);
- Deriving key information from a key or password associated with the Mobile Node (fig. 6, ref. num S6-3); and
- Sending a reply message to the Home Agent, the reply message including the key information associated with the Mobile Node, thereby enabling the Home Agent to derive a shared key to be shared between the Mobile Node and the Home Agent from the key information (fig. 6, ref. num S6-4 and S6-5);
- **Wherein the reply message does not include the shared key to be shared between the Mobile Node and the Home Agent (fig. 7).**

Regarding claim 2, Yokote teaches wherein deriving key information comprises deriving the key information from a second set of key information derived from the key of password (paragraph 0062).

Regarding claim 3, Yokote teaches wherein deriving key information comprises obtaining the derived key information from a domain controller or server (fig. 5-7, the ticket granting server).

Regarding claim 4, Yokote teaches wherein the request message is an access request message and the reply message is an access reply message (paragraph 0060).

Regarding claim 5, Yokote teaches wherein the key or password comprises a Windows password associated with the Mobile Node (fig. 6, ref. num S6-1).

Regarding claim 6, Yokote teaches further comprising obtaining the key or password from a domain controller (fig. 5-7, ticket granting server).

Regarding claim 7, Yokote teaches wherein obtaining the key or password from the domain controller comprises:

- Sending a request to the domain controller for the key or password associated with the Mobile Node; and receiving the key or password associated with the Mobile Node from the domain controller (fig. 6, ref. num S6-1, the user is required to enter and send the user name).

Regarding claim 8, Yokote teaches further comprising applying the key information to authenticate the request message (fig. 6).

Regarding claim 9, Yokote teaches wherein the key or password is stored at the Mobile Node, thereby enabling the Mobile Node to derive the key information from the key or password (paragraph 0069, the SIM of the Mobile Node stores the key).

Regarding claims 10 and 48-50, Yokote teaches in a Home Agent supporting Mobile IP, a method/computer-readable medium/Home Agent of authenticating a Mobile Node, comprising:

- Receiving a **Mobile IP** registration request from a Mobile Node, the **Mobile IP** registration request identifying the Mobile Node (fig. 6, ref. num S6-1);
- Sending a request message to a AAA server, the request message identifying the Mobile Node (fig. 6, ref. num S6-2);
- Receiving a reply message from the AAA server, the reply message including key information associated with the Mobile Node (fig. 6, ref. num S6-3);
- Deriving a key from the key information, the key being a shared key between the Mobile Node and the Home Agent (fig. 6, ref. num S6-4); and
- Sending a **Mobile IP** registration reply to the Mobile Node, **wherein the Mobile IP registration reply does not include the key** (fig. 6, ref. num S6-5 and fig.7).

Regarding claim 13, Yokote teaches wherein deriving the key and sending the **Mobile IP** registration reply to the Mobile Node are performed when the reply message received from the AAA server indicates that the Mobile Node is successfully authenticated (fig. 7 takes place after fig. 6 authenticates the Mobile Node).

Regarding claim 14, Yokote teaches wherein the request message is an access request message and the reply message is an access reply message (paragraph 0060).

Regarding claim 15, Yokote teaches wherein the Mobile Node is to derive the shared key from a second set of key information stored at the Mobile Node (paragraph 0061).

Regarding claim 16, Yokote teaches wherein the key information is equivalent to the second set of key information (paragraph 0061).

Regarding claim 17, Yokote teaches wherein the second set of key information stored at the Mobile Node is a root key, a password, or a key shared between the Mobile Node and the Home Agent in a previous session (paragraph 0057).

Regarding claims 18 and 39, Yokote teaches wherein the registration request includes a SPI, replay protection timestamp, and indicates an algorithm to be used to authenticate the registration request, wherein the SPI, the replay protection timestamp, and the algorithm are associated with the key information (fig. 8).

Regarding claim 19, Yokote teaches further comprising installing the derived key, the SPI, the replay protection timestamp, and the algorithm in a security association (paragraph 0049).

Regarding claims 20 and 40, Yokote teaches wherein the registration reply includes a SPI, replay protection timestamp, and indicates an algorithm to be used to

Art Unit: 2136

authenticate the registration replay, wherein the SPI, the replay protection timestamp, and the algorithm are associated with the key information (fig. 8).

Regarding claim 21, Yokote teaches wherein the **Mobile IP** registration reply indicates that the Mobile Node is to derive the shared key between the Mobile Node and the Home Agent (fig. 6, ref. num S6-3).

Regarding claims 22 and 42, Yokote teaches wherein at least one of the presence of one or more extensions in the **Mobile IP** registration reply and an SPI in the **Mobile IP** registration reply indicates that the Mobile Node is to derive the shared key between the Mobile Node and the Home Agent (paragraph 0048).

Regarding claims 23 and 43, Yokote teaches wherein the **Mobile IP** registration request indicates that the Home Agent is to derive the shared key between the Mobile Node and the Home Agent from a second set of key information received by the Home Agent (fig. 6, ref. num S6-3).

Regarding claims 24 and 44, Yokote teaches wherein at least one of the presence of one or more extensions in the **Mobile IP** registration request and an SPI in the **Mobile IP** registration request indicates that the Home Agent is to derive the shared key between the Mobile Node and the Home Agent (paragraph 0048).

Regarding claim 25, Yokote teaches wherein the presence of an authentication protocol extension in the **Mobile IP** registration request indicates a protocol to be used to authenticate the **Mobile IP** registration request and derive the shared key (paragraph 0049).

Regarding claim 26, Yokote teaches wherein the presence of a session key extension and derived session key extension in the registration request indicates that both a session key and a derived session key are to be generated and installed (paragraph 0049).

Regarding claim 27, Yokote teaches further comprising receiving a subsequent **Mobile IP** registration request from the Mobile Node to refresh the derived session key (paragraph 0009).

Regarding claim 28, Yokote teaches further comprising authenticating the subsequent **Mobile IP** registration request using the session key (fig. 6).

Regarding claim 29, Yokote teaches further comprising sending a subsequent **Mobile IP** registration reply to the Mobile Node including the derived session key extension, wherein the **Mobile IP** registration reply is to be authenticated by the Mobile Node using the session key (fig. 6, ref. num S6-4).

Regarding claim 30, Yokote teaches wherein the key information is a previously used session key shared between the Mobile Node and the Home Agent (paragraph 0057).

Regarding claim 31, Yokote teaches wherein the key information is derived from a password associated with the Mobile Node (paragraph 0061).

Regarding claim 32, Yokote teaches wherein the password is a Windows password (fig. 6, ref. num S6-1).

Regarding claim 33, Yokote teaches further comprising deriving a subsequent key from the shared key (paragraph 0050).

Regarding claim 34, Yokote teaches wherein deriving the subsequent key from the shared key is performed when a binding associated with the Mobile Node is cleared (paragraph 0009-0012).

Regarding claim 35, Yokote teaches wherein the binding associated with the Mobile Node is cleared upon expiration of the lifetime of the Mobile Node or deregistration of the Mobile Node (paragraph 0009-0012).

Regarding claims 36 and 51-53, Yokote teaches in a Mobile Node, a method/computer-readable medium/mobile node of registering with a Home Agent supporting Mobile IP, comprising:

- Sending a registration request to the Home Agent (fig. 6, ref. num S6-2);
- Receiving a registration reply from the Home Agent, the registration reply indicating that the Mobile Node is to derive a key to be shared between the Mobile Node and the Home Agent, **wherein the registration reply does not include the key to be shared between the Mobile Node and the Home Agent** (fig. 6, ref. num S6-4 and fig. 7); and
- Deriving a key to be shared between the Mobile Node and the Home Agent from the key information stored at the Mobile Node (fig. 6, ref. num S6-5).

Regarding claim 38, Yokote teaches wherein the key information is a root key, a password, or a key shared between the Mobile Node and the Home Agent in a previous session (paragraph 0061, session key).

Regarding claim 41, Yokote teaches wherein the registration reply indicates whether the Mobile Node is to derive the shared key between the Mobile Node and the Home Agent, the method further comprising:

- Determining from the registration reply whether the Mobile Node is to derive the key; wherein deriving a key is performed when it is determined from the registration reply that the Mobile Node is to derive the key (paragraph 0061).

Art Unit: 2136

Regarding claim 54, Yokote teaches wherein deriving key information from a key or password associated with the Mobile Node includes deriving the key information from a password, wherein the key information is not derived from a key (paragraph 0061).

Claim Rejections - 35 USC § 103

5. Claims 11, 12, and 37 are rejected under 35 U.S.C. 103(a) as being unpatentable over Yokote (USPGPUB 2002/0147820) in view of Abrol et al. (U.S. Patent No. 6,785,823).

Regarding claims 11, 12, and 37, Yokote teaches all the limitations of claims 10 and 36, above. However, Yokote does not teach challenge response.

Abrol et al. teaches wherein the **Mobile IP** registration request includes a CHAP challenge and response (fig. 2).

It would have been obvious to one of ordinary skill in the art, at the time the invention was made, to combine CHAP, as taught by Abrol et al., with the method of Yokote. It would have been obvious for such modifications because CHAP allows a mobile device to perform authentication (see col. 2, lines 52-55 of Abrol et al.).

Regarding claim 12, Yokote as modified by Abrol et al. teaches wherein deriving a key from the key information comprises deriving the key from the key information and

a CHAP challenge and response obtained from the **Mobile IP** registration request (see fig. 2 of Abrol et al.):

Regarding claim 37, Yokote as modified by Abrol et al. teaches wherein deriving a key from the key information comprises deriving the key from the information and a CHAP challenge and response obtained from the registration reply (see fig. 2 of Abrol et al.).

Response to Arguments

6. Applicant argues that Yokote does not teach the newly amended features, that is, Yokote does not teach wherein the reply message does not include the shared key to be shared between the Home Agent and the Mobile Node.

Yokote teaches, at figure 6, that an authentication request is made by a first entity. A response is sent back from a second entity that includes a ticket and session key, both encrypted using a secret key of the first entity. At this point, the first entity uses its secret key to decrypt the encrypted ticket and session key. It is only after the decryption step that the session key can be used by the two entities. Therefore, the reply message, sent from the second entity to the first entity, does not include the shared key, but rather encrypted data that is unintelligible by the entities until a proper decryption takes place.

Conclusion

7. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire **THREE MONTHS** from the mailing date of this action. In the event a first reply is filed within **TWO MONTHS** of the mailing date of this final action and the advisory action is not mailed until after the end of the **THREE-MONTH** shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than **SIX MONTHS** from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Brandon S. Hoffman whose telephone number is 571-272-3863. The examiner can normally be reached on M-F 8:30 - 5:00.


If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Nasser G. Moazzami can be reached on 571-272-4195. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Brandon Hoffman/

BH

NASSER MOAZZAMI
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100


8,141,07